19. Examine in brief about Message Authentication Code with example.

20. Explain in detail about Pretty Good Privacy in Electronic Mail Security with neat diagram.

———————

NOVEMBER/DECEMBER 2025

FECA63B/FECS63B/CECA63B/CECS63B — CRYPTOGRAPHY

Time : Three hours Maximum : 75 marks

SECTION A — (10 × 2 = 20 marks)

Answer ALL questions.

1. Define Data Integrity.

2. What is meant Digital Signature?

3. Explain about Secret Key.

4. Extend about Polyalphabetic Ciphers.

5. Plan in detail about Backward Compatibility in Key Management.

6. Analyze about Man-in-the-middle attack in Key Management with example

7. Explain about Content Modification in Authentication Requirements.

8. Examine in brief about the Message Encryption in Authentication Functions.

9. Conclude about Masquerader in Intruders.

10. Construct about Clandestine user in Intruders.

SECTION B — (5 × 5 = 25 marks)

Answer ALL questions.

11. (a) Relate in detail about Security Trends with example.

Or

(b) Interpret in brief about Model for Network Security with neat diagram.

12. (a) Discuss in detail about steganography.

Or

(b) Demonstrate in detail about AES Cipher with neat diagram.

13. (a) Explain preudo random number generation in detail.

Or

(b) Develop in brief about Elliptic Curves over Real Numbers in Elliptic Curve Arithmetic with example.

14. (a) Examine in brief about HMAC with example.

Or

(b) Survey in detail about CMAC with example.

15. (a) Determine in detail about Internet Mail Architecture in Electronic Main Security with neat diagram.

Or

(b) Discuss in brief about Password Management with example.

SECTION C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Show in detail about OSI Security Architecture with neat diagram.

17. Summarize in brief about Differential and Linear Cryptanalysis with example.

18. Construct in detail about Description of RSA Algorithm with example.

19. Examine in brief about Message Authentication Code with example.

20. Explain in detail about Pretty Good Privacy in Electronic Mail Security with neat diagram.

———————

NOVEMBER/DECEMBER 2025

FECA63B/FECS63B/CECA63B/CECS63B — CRYPTOGRAPHY

Time : Three hours Maximum : 75 marks

SECTION A — (10 × 2 = 20 marks)

Answer ALL questions.

1. Define Data Integrity.

2. What is meant Digital Signature?

3. Explain about Secret Key.

4. Extend about Polyalphabetic Ciphers.

5. Plan in detail about Backward Compatibility in Key Management.

6. Analyze about Man-in-the-middle attack in Key Management with example

7. Explain about Content Modification in Authentication Requirements.

8. Examine in brief about the Message Encryption in Authentication Functions.

9. Conclude about Masquerader in Intruders.

10. Construct about Clandestine user in Intruders.

SECTION B — (5 × 5 = 25 marks)

Answer ALL questions.

11. (a) Relate in detail about Security Trends with example.

Or

(b) Interpret in brief about Model for Network Security with neat diagram.

12. (a) Discuss in detail about steganography.

Or

(b) Demonstrate in detail about AES Cipher with neat diagram.

13. (a) Explain preudo random number generation in detail.

Or

(b) Develop in brief about Elliptic Curves over Real Numbers in Elliptic Curve Arithmetic with example.

14. (a) Examine in brief about HMAC with example.

Or

(b) Survey in detail about CMAC with example.

15. (a) Determine in detail about Internet Mail Architecture in Electronic Main Security with neat diagram.

Or

(b) Discuss in brief about Password Management with example.

SECTION C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Show in detail about OSI Security Architecture with neat diagram.

17. Summarize in brief about Differential and Linear Cryptanalysis with example.

18. Construct in detail about Description of RSA Algorithm with example.